Health Informatics Journal

Article

Health Informatics Journal
16(3) 211–223

DOI: 10.1177/1460458210377482
http://jhi.sagepub.com
SAGE

Securing the communication of medical information using local biometric authentication and commercial wireless links*

Vladimir I. Ivanov
University of Maryland, College Park, MD, USA

Paul L. Yu
US Army Research Laboratory, Adelphi, MD, USA

John S. Baras
University of Maryland, College Park, MD, USA

Abstract

Medical information is extremely sensitive in nature – a compromise, such as eavesdropping or tampering by a malicious third party, may result in identity theft, incorrect diagnosis and treatment, and even death. Therefore, it is important to secure the transfer of medical information from the patient to the recording system. We consider a portable, wireless device transferring medical information to a remote server. We decompose this problem into two sub-problems and propose security solutions to each of them: (1) to secure the link between the patient and the portable device, and (2) to secure the link between the portable device and the network. Thus we push the limits of the network security to the edge by authenticating the user using their biometric information; authenticating the device to the network at the physical layer; and strengthening the security of the wireless link with a key exchange mechanism. The proposed authentication methods can be used for recording the readings of medical data in a central database and for accessing medical records in various settings.

Keywords

authentication, biometrics, communication, cryptography, physical layer

Introduction

Medical information is extremely sensitive in nature. A compromise, such as eavesdropping or tampering by a malicious third party, may result in identity theft, incorrect diagnosis and treatment,

*This work was presented at the Proceedings of the 14th International Symposium for Health Information Management Research at Kalmar in October 2009 by Ivanov VI, Yu PL, and Baras JS.

Corresponding author:
John S. Baras, University of Maryland, College Park, MD 20742, USA
Email: baras@umd.edu

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Securing The Communication Of Medical Information Using Local Biometric Authentication And Commercial Wireless Links	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Research Laboratory,Adelphi,MD,20783**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Health Informatics Journal, Volume 16, Number 3, pp. 211-223, September 2010

14. ABSTRACT
Medical information is extremely sensitive in nature ? a compromise, such as eavesdropping or tampering by a malicious third party, may result in identity theft, incorrect diagnosis and treatment, and even death. Therefore, it is important to secure the transfer of medical information from the patient to the recording system. We consider a portable, wireless device transferring medical information to a remote server. We decompose this problem into two sub-problems and propose security solutions to each of them: (1) to secure the link between the patient and the portable device, and (2) to secure the link between the portable device and the network. Thus we push the limits of the network security to the edge by authenticating the user using their biometric information; authenticating the device to the network at the physical layer; and strengthening the security of the wireless link with a key exchange mechanism. The proposed authentication methods can be used for recording the readings of medical data in a central database and for accessing medical records in various settings.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

and even death. The misuse of a stolen identity for receiving healthcare may result in unexpected bills and, still worse, doctors may make incorrect diagnoses and apply deleterious treatments based on data from the identity thief's medical history.[1] The application of wireless sensor networks to healthcare systems and their integration with the conventional wireless communication networks creates new opportunities, such as automatic collection of readings of medical sensors, and new challenges, with security and data confidentiality being critical.[2, 18] One platform for building sensor networks for medical care, including hardware and software implementations, that bridges the gap between the existing sensor network systems and the requirements of healthcare is proposed by Shnayder et al.[3] A shortcoming, however, is its lack of security, both as authentication and as data protection. Another framework for remote home healthcare using GSM/GPRS has been proposed,[4] but it uses passwords for authentication, does not make any security analysis, and does not propose a solution for the security weakness of Bluetooth. Other architectures require public key infrastructures for authentication[5] or impose constraints on clock accuracy/synchronization,[6] either of which is undesirable. And finally, the use of asymmetric keys is particularly problematic in energy-constrained and computationally limited systems.

An interesting architecture and implementation that address the specific challenges in securing a wireless medical sensor network have been described[7], where the authors propose using biometric (fingerprint) and medical (ECG) information for authentication and elliptic curve public-key cryptography for establishing symmetric shared keys for data protection. Transferring a user's biometric and medical information over a wireless network and storing this information in each base station, however, are problematic: a security compromise may have grave consequences as this type of information cannot be revoked. On the other hand, since the biometric information cannot be assumed to be secret, an attacker who captures a mote and has a user's biometrics can impersonate the mote to the base station since the mote authentication is essentially done with the user's biometrics (the motes do not have public key pairs). Moreover, each base station has to store the biometric and medical information, used for authentication, of all users, which poses considerable challenges for system update and scalability. In addition, using medical data (from the sensor) as a second-tier authentication is problematic because the monitored data are often pathological (i.e. revealing disease symptoms) and therefore may lead to unacceptably high false reject rate, thus disabling the communication altogether. Finally, ECG is also sensitive to body condition, and when used for authentication, the technology is commercially immature and relatively inaccurate.

An important objective in securing such networks is using commercially available solutions and requiring as little modification of the communication infrastructure as possible, because the additional cost of the security solution can be a major obstacle for its mass adoption and deployment.

We consider the scenario where a user, e.g. the patient, has a portable, wireless medical device that is able to transfer medical information to a network access point. We decompose this problem into two subproblems and propose our solutions in turn: (1) to secure the link between the user and the portable device, and (2) to secure the link between the portable device and the network access point.

We take the general view that data confidentiality is ensured by using cryptography. The conventional approach is to employ a symmetric key with appropriate length as this method is fast and provides strong protection. However, encryption and decryption alone do not provide authentication, i.e. verification of the claim about the identity (of a human or a system). Authentication is a critical element in the security link because, if done improperly, it may lead to data transfer from an unauthentic sender or to an unauthentic recipient.

In this article, we consider the authentication problem at two interfaces: between the user and the portable device, and between the portable device and the network access point (or a remote server). Clearly, these two problems lie in different domains – the first is a human-to-machine

Figure 1. Authentication in two steps

authentication, while the second is a machine-to-machine authentication – and each requires a different approach. The novelty of our work is twofold. First, by using a biometric authentication, we effectively 'push' the boundary of the authentication not only from the network to the device, but all the way to the end user. Second, with a recent breakthrough at the physical layer of communication and in the cryptographic technology, we can vastly improve previously insecure communication links between the device and the network.

Authentication in two steps

We propose to split the authentication of a user to a network access point in two steps (see Figure 1). We use biometric information for the human-to-machine authentication. For the machine-to-machine authentication, we propose a novel approach at the physical layer. We also propose to strengthen the security of a popular wireless link using a fast and efficient method for key exchange.

Local biometric authentication

In the context of information technologies, biometrics is measuring, analysing, and using physiological and behavioural traits for identifying individuals. Biometrics has been used for automated authentication of people to systems for over a decade, making the authentication more convenient as it does not require memorizing passwords or PIN codes. This convenience is particularly important in healthcare applications as the medical information may be time critical and may need to be communicated even when the patient is under mental distress or physically unable to enter passwords or PIN codes. Furthermore, to be universally acceptable, a technology also has to be easy to use by people without specific technical training, in particular by seniors and children. Although easy to use, the RFID alternative and its derivatives cannot provide the required secure identification and authentication of humans because the RFID tags can be easily replaced (or their content changed) unless they are implantable, which at this stage is inapplicable for numerous reasons (e.g. public acceptance, policy, health concerns, security weaknesses and cost).

Today, many low-cost and small-sized systems for biometric authentication are commercially available and have the potential to become ubiquitous. Using biometrics for authentication, however, is problematic because the biometric information has a low degree of secrecy, i.e. it can easily be captured by an unintended recipient, which may occur even without the consent of the user.[9] The stolen information may be used to construct counterfeited or artificial biometrics, which has been shown to be relatively easy.[10] The compromise of an individual's biometric information may have graver consequences than the compromise of a password. For example, in contrast to passwords, biometric characteristics are not easily changeable and cannot be revoked, e.g. altering the person's fingerprint or iris cannot be done without surgical methods. In addition to the chronic security weaknesses of commonplace computer systems, function creep and owner abuse result in security breaches which are even harder to detect and thwart. Thus, storing the biometric information on a local computer, sending it over a network, and/or storing it on a remote server, even in encrypted form, would only further compound the problem. With over 260

million records, containing personal information such as Social Security numbers, account numbers and driver's licence numbers, compromised due to security breaches since January 2005 in the US alone,[11] assuming that the biometric information can remain secret is clearly wrong. Furthermore, a recent investigation by Associated Press revealed that 'banks and other companies that handle your information are not being nearly as cautious as they could', which results in 'gambling with your personal data' once you pay with a credit card.[12] Under such circumstances, people's mistrust of the ability of systems and networks to protect their confidential information is completely justified.

We therefore propose to use biometric information to authenticate the user to a portable device; this device is the user's personal property and is in the user's possession all of the time. We call this authentication *local authentication*. Thus, the biometric information is kept only in the device, not in a computer or a server on the network, and is locked onto the device. The locking is implemented using special hardware which ensures that the stored information cannot be compromised because the hardware inherently offers a higher degree of security. The device essentially becomes 'an extension' of the user and can be carried by the user at all times. Moreover, this approach requires few or no changes to the infrastructure, in particular, no modification of the security protocols for authentication of a device to a network. It also relaxes the expectations and assumptions about the trustworthiness of the user from the point of view of the network. And finally, the local authentication is capable of 'hiding' the identity (e.g. the real name of the user) as it naturally shields the personal information from being sent over the network (or can instead use an identification number) without the need for additional network infrastructure, such as a trusted third party, as proposed elsewhere.[13]

Besides the purely technical arguments, the proposed method also helps gain the confidence of users perceptually and psychologically. Users want to use a technology they are comfortable with but do not want to understand how exactly it works. For example, a patient knows that the biometric authentication works in other authentication scenarios, e.g. when appearing in person in a doctor's office. Now the patient is using her biometrics locally to authenticate to her doctor, which 'brings' the doctor right 'in front of her'. Therefore, in addition to the technical guarantee about preserving the secrecy of the biometric information that our approach gives, it also makes the user more readily accept, and therefore take advantage of, the medical device, enabling the doctors and medical staff to provide better healthcare.

For biometrics, we propose to use fingerprints. Human fingerprint patterns are highly distinct, develop early in life, and are relatively permanent.[14] Fingerprints have been used for identifying individuals for over a century. Initially systematized and developed for law enforcement, today fingerprints are widely used for access to facilities and for authentication to computer systems. Furthermore, low-cost and small-sized implementations of fingerprint sensors are available, making authentication based on fingerprints particularly suited for portable devices.

Portable handheld devices have been increasingly used in a diverse set of applications: for communication (e.g. cell and smart phones), as personal data assistants (PDAs), and for access to financial services (e.g. hardware tokens). These devices have seen a long evolution in the access control over them: from not being protected at all, to passwords or PIN codes, to modern biometric authentication, with the most ubiquitous being fingerprint authentication.[15, 16]

A major challenge for the biometric authentication in our scenario (Figure 1) is that the authentication may take place in an unsupervised environment and at the user's convenience (e.g. at home). Thus, because the biometric information is not secret, an attacker who may have obtained the biometric information of the legitimate user will be able to provide it to the biometric sensor as a counterfeit. Another problem arises from the portability of the device: it may be easily stolen, giving the attacker physical access to the device and thus the ability to launch a powerful attack.

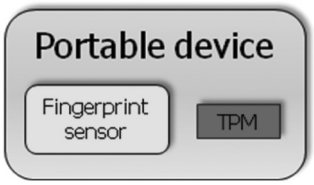

Figure 2. The portable device with a fingerprint sensor and a TPM

Fortunately, recent work on detecting fake fingerprints[17] and detecting attacks on the fingerprint sensor have yielded to promising results.

To protect the confidentiality of the biometric information, we propose to use a Trusted Platform Module (TPM)[19], specified by the Trusted Computing Group (TCG). The TPM is a 'locked-down' architecture that protects the integrity and confidentiality of the data with hardware support using cryptographic keys built into the hardware. We propose to incorporate the TPM in the portable device (see Figure 2) and protect the biometric information in the TPM or store it in the device, but first encrypt it with keys managed by the TPM. The biometric information also never leaves the device. Our current research includes studying various methods for using the TPM to secure the storage of the user's biometrics. The TPM also identifies the device, performs integrity measurements and reports them via a mechanism called attestation. For example, the TPM can attest to the software running in the device and securely communicate this information to a remote server. Although a commercially available solution that combines a fingerprint authentication with a TPM to increase the security of a computer system is available,[20] currently it uses a wired interface (USB) to connect to the computer; and, because its design is proprietary, the mechanism for protecting the biometric information implemented in the device is not publicly available.

The biometric information can be also securely stored into the smart chip of a smartcard;[15] the smartcard is also the property of the user and is inserted into the portable device for performing the local authentication. Although the degree of tamper resistance of the smartcards is typically lower than that of the TPM, a smartcard provides greater flexibility as the biometric information can be stored in a single smartcard which can then be used in many portable devices.

We again stress the fact that it is this hardened security that encourages the use of the device. Very often new technologies are not adopted because users do not trust them and/or fear invasion of their privacy or theft of their private information.

Authentication of a portable device to a network access point or to a remote server

Just as the user has to be authenticated and the portable device has to be secure, the communication from the device to a network access point or to a remote server has also to be secure. Also similarly to the biometric authentication, which uses inherent characteristics of humans, physical layer techniques, developed recently, exploit radio frequency characteristics to uniquely identify devices.

The conventional mechanisms for device-to-network authentication are three: handshaking protocols (e.g. Kerberos), digital signatures or certificates (e.g. X.509), and symmetric authentication (e.g. message authentication codes, MACs). The handshaking protocols, however, require coordination, use extra bandwidth or cause delay, generally are computationally expensive, and require a central authority. Digital signatures or certificates also require a central authority and are computationally expensive because of the use of asymmetric cryptography. Symmetric authentication methods are more computationally efficient, but they assume prior key distribution.

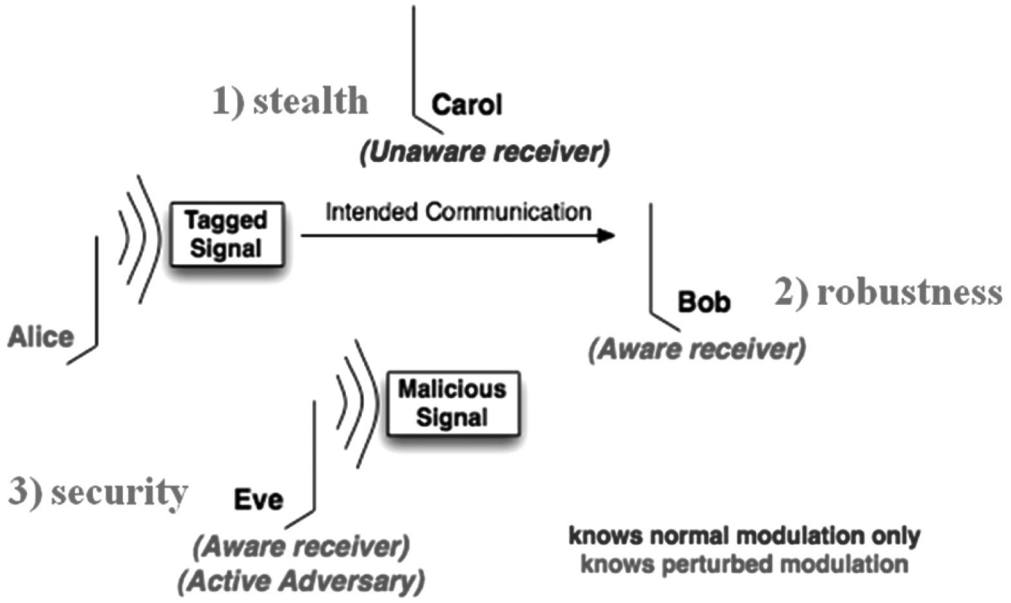

Figure 3. Physical-layer authentication using perturbed modulation

The key innovative idea, proposed elsewhere,[8, 21, 22] is to artificially embed a stealthy 'fingerprint' – a tag – into the modulation waveforms communicated between the two parties (Alice and Bob in Figure 3). Alice uses this perturbed modulation scheme and wants to authenticate to Bob. The third parties, Carol and Eve, are the adversaries. The waveforms are perturbed in such a way as to ensure three properties: (1) stealth, (2) robustness and (3) security. Carol is not aware that the waveforms are perturbed and she is unable to detect this; this is *stealth* or unnoticeable presence. Eve knows that the modulation is perturbed but still cannot detect the presence of the authentication, modify Alice's messages or impersonate Alice; this is *security*, i.e. resistance to attacks. Bob can reliably authenticate Alice in the presence of noise and interference; this is *robustness*, i.e. the perturbed modulation is resistant to noise and interference.

This technique has been shown to offer high security while at the same time remaining transparent to the existing communication technologies. Since this authentication is implicit to the device, the authentication adds to, rather than replaces, existing security measures. Thus, by combining our techniques with the currently used security methods, i.e. MAC and device authentication numbers, we significantly strengthen several aspects of the security of the device.

In the same vein of increasing security, we also demonstrate how another recently developed security mechanism can strengthen the security of the wireless link: the Markov model-directed key exchange method.[8, 23, 24] This method uses synchronized Markov models to direct the key exchange between two parties.[23] Assume that initially the portable device and the network access point (or the remote server) are paired by using a shared secret key. The general idea is that when two parties share the same model, they can exchange and replace keys very rapidly while remaining synchronized. However, an attacker without the correct model will be unable to find out which key is being used. Therefore, the ability to find the correct keys is unique to the authentic parties. Although we assume some type of key bootstrapping (e.g. via the initial key distribution), our method for key update is simpler, faster and more

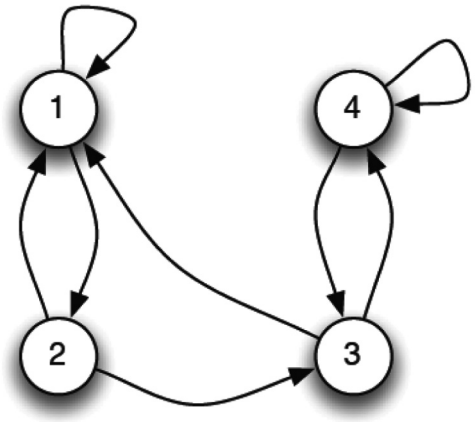

Figure 4. A Markov model: states and transitions among them

efficient than the conventional methods for key agreement using messages, in particular the method proposed by MacDonald.[25]

A Markov chain is a random process where the future depends only on the present and not on the past; therefore, the present fully captures all the information that influences the future evolution of the process. The chain consists of states and the transitions among them (see Figure 4); in our case, each state represents a key and each transition indicates the possibility to change from the first key to the second one, e.g. from key 3 to key 1 (see Figure 4). Thus, the sequence of keys 1, 2 and 3 is valid, but the sequence of keys 1, 2 and 4 is invalid because there is no direct transition between key 2 and key 4.

Here we detail the algorithm for Markov model-directed key exchange. Suppose that there are two parties and that in our scenario Alice denotes the portable device and Bob denotes the network access point. Assume that Alice and Bob have already agreed on a secret master key K_m that determines a Markov model and has initial state K_0.

1 Alice uses K_m to select a Markov model MM_A.
Alice generates a random seed N_1.
Alice uses MM_A to select a key K_1.
Alice sends $E_{K1}(N_1)$ to Bob; $E_{K1}(N_1)$ is N_1 encrypted with key K_1.

2 Bob uses K_m to select a Markov model MM_B.
Bob uses MM_B to generate possibilities for the key K_1.
Bob decrypts $E_{K1}(N_1)$ and verifies the decryption of N_1.
IF the decryption integrity check fails:
THEN halt. Since Bob is unable to decrypt $E_{K1}(N_1)$, then Bob knows he doesn't have the same K_m as Alice and the authentication fails.
ELSE continue.

At this point, Bob can verify the authenticity of Alice because Bob is able to decrypt correctly the encrypted nonce N_1. This signals that Alice is using the same master key as Bob is using to generate the keys. However, Alice does not know if Bob is authentic or not. Therefore, Alice needs to wait to see if Bob uses the correct key to encrypt the message that Bob will send. Thus:

Bob uses K_1 and MM_B to select a key K_2.
Bob generates a random nonce N_2.
Bob sends $E_{K2}(N_2)$ to Alice.

3 Alice uses K_1 and MM_A to select possibilities for the key K_2.
Alice decrypts $E_{K2}(N_2)$ and verifies the decryption of N_2.
IF the decryption integrity check fails:
THEN halt. Since Alice is unable to decrypt $E_{K2}(N_2)$, Alice knows that Bob is using a different K_m and the authentication fails.
ELSE continue.

At this point, Alice can verify the authenticity of Bob because Alice is able to decrypt correctly the encrypted nonce N_2. This signals that Bob is using the same master key K_m as Alice is to generate the keys. Now both parties have authenticated each other and the secure communication can begin.

Once the handshaking is complete, the secret keys are periodically refreshed automatically to harden the link security.[8, 23, 24] The timeline of the algorithm is shown in Table 1.

We propose using the Markov model-directed key exchange method to strengthen the security of a commercially available wireless link for portable devices that is very well suited for pervasive healthcare applications, particularly in medical telemetry such as Bluetooth.[26] This is a popular standard for low-cost devices that boasts low power and relatively high high data rate for short distances. However, its authentication protocol has a serious flaw and is notoriously weak. The main problem stems from the random nonces that are transmitted without encryption in the 'mutual authentication' phase of the pairing process. To generate the initial shared key between Alice, denoting the portable device, and Bob, denoting the network access point, a PIN code is combined with a nonce (see Figure 5). The nonce is transmitted to the other side without encryption, which can be defeated with a 'known plaintext' attack. In order to thwart this attack, we propose to encrypt the nonces before they are sent. A Markov key exchange method allows this to be done securely.

Table 1. Timeline of the Markov model-directed key exchange algorithm

Time	Alice	Communication	Bob
	K_m	← Shared →	K_m
0	Sends $E_{K1}(N_1)$	→	
1			Finds K_1 to verify
2		←	Sends $E_{K2}(N_2)$
3	Finds K_2 to verify		

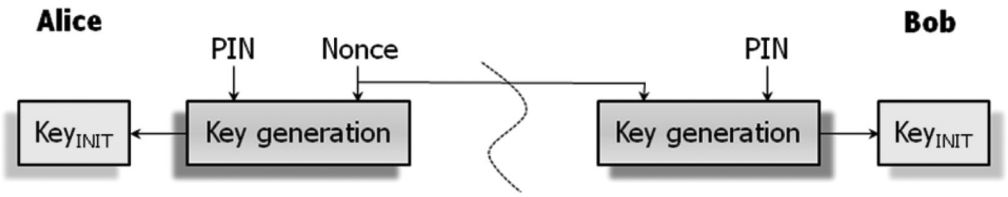

Figure 5. Initial key generation in Bluetooth

The network access point needs to first ensure that the legitimate user is using the portable device. Therefore, no communication is permitted until the local biometric authentication is completed successfully. For example, if an attacker steals the portable device, no medical information will be transferred or requested until the genuine fingertip is applied to the biometric sensor.

Use cases

In this section, we first summarize the main advantages of our approach and then suggest two groups of applications for the methods we propose.

Using biometrics for human authentication to a portable device is easier than using passwords or PIN codes as users (patients) need not memorize anything, need not have computer skills and can authenticate even when under mental distress or physically unable to type. The local authentication limits the spread of biometric information by 'locking it' in the device and never sending it to a computer or over a network, which significantly reduces the risk of compromising the biometric data. Furthermore, the security of a simple device (such as a PDA) is much easier to ensure than that of a computer, which typically runs many and diverse applications in a general-purpose operating system. Physically possessing the portable device all of the time increases the user's confidence in the control of their private information, which makes the adoption of the technology easier. Finally, the intermediating portable device naturally allows hiding the user's personal information, including their real name, and prevents it from ever being sent to the network, thus enabling the delivery of anonymous services. As for the device-to-network authentication and security, our approach does not require a public key infrastructure and relies on physical layer techniques that inherently provide higher security. The efficiency of the key exchange mechanism allows simple implementations.

Figure 1 shows the two steps of the authentication process. Once the authentication is successful, secure information exchange between the user and the remote server may begin. The confidentiality and integrity of the data being transferred from this moment onward can be ensured by using secure protocols of higher levels, e.g. SSL or IPsec. Depending on the functionality of the portable device and the particular applications, the user may, for example, enter and read textual or graphical information, type their username (in the system) and request data to be retrieved from a remote server. We, however, do not discuss such details as they are not directly related to the problem of securing the communication at low level, i.e. by using biometric information and physical layer techniques. Thus, the suggested use cases only conceptually illustrate the two groups of applications.

Recording the readings of medical sensors in a central database

Suppose, for example, that a patient has a sensor for monitoring blood pressure or heart rate, and that the data are sent to a remote database server that records them and provides them to a physician for determining a diagnosis. The data may need to be recorded over a long period (e.g. over a month) and to be collected at any time of the day, including overnight. The medical sensor sends the data (locally) to the portable device, from which the data are transferred to a network access point and then to a remote server. The portable device should be able to authenticate first to the network access point and then to a remote server, and securely (i.e. using encryption) transfer the data to it. The first step is authenticating the user to the device, and the second is authenticating the device to the network access point.

The medical sensor can, for example, read the data and send them to the portable device, which in turn can store them in its local memory. After the user authenticates to the device, the data

transmission to the network access point is authorized, and the data are sent to the network. In this scenario, the patient has full control over the time when the medical data are transferred. In another scenario, it may be required that the measured data are sent immediately, in which case the patient can authenticate to the device only once, at the beginning, and can grant permission that the future transmissions take place automatically, without performing additional biometric authentications every time a piece of data is ready to be sent.

An exemplar application is the service-based architecture WASP (Wirelessly Accessible Sensor Populations) for pervasive monitoring of elderly people,[27] where the proposed biometric authentication takes place in the personal mobile hub (PMH) and the proposed methods for increasing the link security are applied between the PHM and the wireless sensor hub. Similarly, another possibility is the system for wearable vital signs monitoring, proposed elsewhere.[28] And finally, the authentication to the mobile phone in particular architectures[29, 30] can be biometrics, and since the communication between the medical sensors and the mobile phone is Bluetooth, our methods for increasing the link security are also applicable. Although we do not assume the presence of a mobile network infrastructure and the functionality it provides, our method for local authentication (and sensor readings) can also be a part of the architecture proposed elsewhere.[5]

Access to medical records in a central database

The proposed methods for authentication can also be used in a small group of nurses and doctors in a medical practice to authenticate users to medical data storage devices such as hard disks. Some hard drives, with very high capacity yet physically small in size, are already equipped with TPMs, which makes the implementation of the proposed authentication methods straightforward. Thus, not only is the access to sensitive information controlled, but at the same time the users are authenticated. The data transferred to the storage devices may include the medical history, current medications, and current readings of the medical sensors on the patient, and can be displayed in an easy-to-read format for fast assessment and action. The method for authentication can also be used in the framework for access to electronic patient records.[31, 32]

Another example application is ‘personal data records’. In conventional ‘electronic data records’, entering and maintaining a patient’s data are the responsibility not of the patient but of someone else, e.g. the insurance company or the doctor. In the personal data record, the patient enters and maintains the data, and therefore the patient must authenticate to the central database and use a secure communication channel to transfer the data (Kaiser Permanente in the US offers a similar service to its members[33]).

Conclusions

The application of wireless sensor networks to healthcare systems and their integration with conventional wireless communication networks create new opportunities and pose new challenges. Because of the very high sensitivity of the medical information, it is important to secure the transfer of medical information from the patient to the system that records and collects it. We propose to split the authentication problem into two authentication steps: of the user to a portable device; and of the device to a network access point (or a remote server).

We propose to use biometrics for the authentication of the user to the portable device. Fingerprints are particularly suited for replacing traditional passwords and PIN codes and provide the convenience and ease of use that are needed in medical applications. To protect the confidentiality of the user’s biometrics, the biometric information is locked down in the portable device using the TPM technology and thus never leaves the device. This essentially makes the device ‘an extension’ of the

user. For authentication of the portable device to the network access point and for strengthening the security of a popular commercial wireless link, we propose to use a physical layer authentication and a Markov key exchange method.

The proposed methods for authentication can be used for recording the readings of medical information to a central database and for access to medical records, in particular for 'personal data records'. The concept of separating the device authentication and the user authentication is also very important for telemedicine. Other applications of the proposed methods, beyond the scope of healthcare, are personal financial/bank services and mobile commerce. As our immediate next step, we consider implementing the proposed methods in a prototype system. Once this is successful, we will study, develop and incorporate the high-level applications, including the appropriate software and communication protocols, which will enable the suggested use cases and allow real trials, i.e. connecting users (patients) with (healthcare) systems.

Acknowledgements

This material is based upon work supported by the Communications and Networks Consortium sponsored by the US Army Research Laboratory under the Collaborative Technology Alliance Program, Cooperative Agreement DAAD19-01-2-0011, and the University of Maryland Foundation. The US Government is authorized to reproduce and distribute reprints for Government purposes, notwithstanding any copyright notation thereon.

Disclaimer

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the US Government.

References

1. Hagberg J. Palm-vein biometrics help accurately ID patients. *SC Magazine*, http://www.scmagazineus.com/Palm-vein-biometrics-help-accurately-ID-patients/article/112054 (2 July 2008, accessed 6 July 2009).
2. Stankovic JA, Cao Q, Doan T, et al. Wireless sensor networks for in-home healthcare: potential and challenges. In: *HCMDSS: High Confidence Medical Device Software and Systems Workshop*, Philadelphia, 2–3 June 2005, p.2–3.
3. Shnayder V, Chen B, Lorincz K, Fulford-Jones TRF, Welsh M. Sensor networks for medical care. In: *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, San Diego, 2 November 2005.
4. Jasemian Y. Security and privacy in a wireless remote medical system for home healthcare purpose. In: *Proceedings of the Pervasive Health Conference and Workshops*, Innsbruck, 29 November to 1 December 2006.
5. Shanmugam M, Thiruvengadam S, Khurat A, Maglogiannis I. Enabling secure mobile access for electronic health care applications. In: *Proceedings of the Pervasive Health Conference and Workshops*, Innsbruck, 29 November to 1 December 2006.
6. Elmufti K, Weerasinghe D, Rajarajan M, Rakocevic V, Khan S. Timestamp authentication protocol for remote monitoring in eHealth. In: *PervasiveHealth 2008: Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare*, Tampere, 30 January to 1 February 2008, p.73–76.
7. Malasri K and Wang L. Design and implementation of a secure wireless mote-based medical sensor network. In: *Proceedings of the 10th International Conference on Ubiquitous Computing*, Seoul, 21–24 September 2008, p.172–181.
8. Yu PL. Physical layer authentication. PhD dissertation, University of Maryland, August 2008.

9. Chaos Computer Club publishes fingerprints of Wolfgang Schäuble, the German Home Secretary. *Heise Online*, http://www.heise.de/english/newsticker/news/105728 (31 March 2008, accessed 6 July 2009).
10. Matsumoto T, Matsumoto H, Yamada K, Hoshino S. Impact of artificial 'gummy' fingers on fingerprint systems. *Proc SPIE* 2002; 4677: 275–289.
11. Privacy Rights Clearinghouse. A chronology of data breaches. http://www.privacyrights.org/ar/ChronDataBreaches.htm (2005–2009, accessed 29 June 2009).
12. Robertson J. Weak security enables credit card hacks. Associated Press, http://tech.yahoo.com/news/ap/20090615/ap_on_hi_te/us_tec_shoppers__gamble (14 June 2009, accessed 6 July 2009).
13. Weerasinghe D, Elmufti K, Rajarajan M, Rakocevic V. Patients' privacy protection with anonymous access to medical services. In: *PervasiveHealth 2008: Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare*, Tampere, 30 January to 1 February 2008, p.127–130.
14. Maltoni D, Maio D, Jain AK, Prabhakar S. *Handbook of fingerprint recognition*. Springer, 2005.
15. National Institute of Standards and Technology. *Study report on biometrics in e-authentication*. INCITS M1/06-0424. Gaithersburg, MD, 15 May 2006.
16. Jansen W, Daniellou R, and Cilleros N. Fingerprint identification and mobile handheld devices: an overview and implementation. NISTIR 7290. Gaithersburg, MD: National Institute of Standards and Technology, March 2006.
17. Tan B and Schuckers S. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In: *CVPRW'06: Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop*, New York, 17–22 June 2006.
18. Dimitriou T and Ioannis K. Security issues in biomedical wireless sensor networks. In: *ISABEL '08: Proceedings of the First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, Aalssborg, 25–28 October 2008.
19. Trusted Platform Module (TPM) specification v1.2. http://www.trustedcomputinggroup.org/developers/trusted_platform_module/specifications.
20. Ultra Mobile Authentication Key (UMAK). Product description. Inaura Inc., http://www.inaura.com.
21. Baras JS, Yu PL, and Sadler BM. Wireless communication method and system for transmission authentication at the physical layer. US patent application, 9 September 2008.
22. Yu PL, Baras JS, and Sadler BM. Physical layer authentication. IEEE Transactions on Information Forensics and Security, March 2008, Volume 3, Issue 1, p.38–51.
23. Baras JS, Yu PL, and Sadler BM. Method and implementation for key generation and replacement using Markov models. US patent application, October 2009.
24. Yu PL, Baras JS, and Sadler BM. Key exchange using Markov models. ACM Transactions on Information and System Security (submitted).
25. MacDonald JA. Cellular authentication and key agreement for service providers. In: *PervasiveHealth 2008: Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare*, Tampere, 30 January to 1 February 2008, p.69–72.
26. Scarfone K and Padgette J. *Guide to Bluetooth security*. Special Publication 800-121, National Institute of Standards and Technology, 3 September 2008. http://csrc.nist.gov/publications/nistpubs/800–121/SP800–121.pdf.
27. Atallah L, Lo B, Guang-Zhong Y, Siegemund F. Wirelessly accessible sensor populations (WASP) for elderly care monitoring. In: *PervasiveHealth 2008: Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare*, Tampere, p.2–7.
28. Chen W, Wei D, Zhu X, et al. A mobile phone-based wearable vital signs monitoring system. In: *CIT 2005: Proceedings of the 5th Conference on Computer and Information Technology*, 21–23 September 2005, p.950–955.

29. Rasid MFA and Woodward B. Bluetooth telemedicine processor for multichannel biomedical signal transmission via mobile cellular networks. IEEE Transactions on Information Technology in Biomedicine, March 2005, Volume 9, Issue 1, p.35–43.
30. Kailanto H, Hyvärinen E, Hyttinen J. Mobile ECG measurement and analysis system using mobile phone as the base station. In: *PervasiveHealth 2008: Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare*, Tampere, p.12–14.
31. Ferreira A, Barreto L, Brandao P, Correia R, Sargento S, Antunes L. A secure wireless architecture to access a virtual electronic patient record. In: *Proceedings of the Pervasive Health Conference and Workshops*, Innsbruck, 29 November to 1 December 2006.
32. Butz A and Kruger A. User-centered development of a pervasive healthcare application. In: *Proceedings of the Pervasive Health Conference and Workshops*, Innsbruck, 29 November to 1 December 2006.
33. HealthcareITNews. Three million people now using Kaiser Permanente's personal health record. http://www.healthcareitnews.com/press-release/three-million-people-now-using-kaiser-permanentes-personal-health-record (22 April 2009, accessed 6 July 2009).